

TABLE OF CONTENTS

I. INTRODUCTION	5
II. OVERVIEW OF THE PATENTS-IN-SUIT.....	6
A. U.S. Patent No. 8,234,705	6
B. U.S. Patent No. 8,965,892	7
III. AGREED UPON CONSTRUCTIONS	8
IV. DISPUTED TERMS AND CONSTRUCTIONS	8
A. U.S. Patent No. 8,234,705	8
i. “trusted platform module”	8
B. U.S. Patent No. 8,965,892	11
i. “electronic document”	11
ii. “document”	15

TABLE OF AUTHORITIES

CASES

<i>Ancora Techs., Inc. v. LG Elecs. Inc.</i> , No. 1-20-CV-00034-ADA, 2020 U.S. Dist. LEXIS 150002 (W.D. Tex. Aug. 19, 2020)	13
<i>Catalina Mktg. Int’l v. Coolsavings.com, Inc.</i> , 289 F.3d 801, 808 (Fed. Cir. 2002)	12
<i>CloudfChange, LLC v. NCR Corp.</i> , No. 6-19-CV-00513-ADA, 2020 U.S. Dist. LEXIS 124625	11
<i>Comark Commc’ns, Inc. v. Harris Corp.</i> , 156 F.3d 1182 (Fed. Cir. 1998)	16
<i>Digital Retail Apps, Inc. v. H-E-B, LP</i> , No. 6-19-CV-00167-ADA, 2020 U.S. Dist. LEXIS 11094 (W.D. Tex. Jan. 23, 2020)	12
<i>Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.</i> , 381 F.3d 1111 (Fed. Cir. 2004)	15
<i>Johnson Worldwide Assocs., Inc. v. Zebco Corp.</i> , 175 F.3d 985	17
<i>Kroy IP Holdings, LLC v. Safeway, Inc.</i> , No. 2-12-CV-800-WCB, 2014 U.S. Dist. LEXIS 102136, 2014 WL 3735222, (E.D. Tex., July 28, 2014)	11
<i>Pisomy v. Commando Constr., Inc.</i> , No. W-17-CV-00055-ADA, 2019 U.S. Dist. LEXIS 31524 (W.D. Tex. Jan. 23, 2019)	17
<i>Sumitomo Dainippon Pharma Co. v. Emcure Pharm. Ltd.</i> , 887 F.3d 1153 (Fed. Cir. 2018)	17
<i>Synqor, Inc. v. Artesyn Tech., Inc.</i> , 709 F.3d 1365 (Fed. Cir. 2013)	10

<i>Thorner v. Sony Computer Entm't Am. LLC</i> , 669 F.3d 1362 (Fed. Cir. 2012)	13
<i>TMI Prods. v. Rosen Entm't Sys., L.P.</i> , 610 F. App'x 968 (Fed. Cir. 2015)	12
<i>Victor Co. of Japan, Inc. v. Intervideo, Inc.</i> , No. A-08-CA-041-SS, 2009 U.S. Dist. LEXIS 133777 (W.D. Tex. July 24, 2009)	12

I. INTRODUCTION

Pursuant to the parties' agreed schedule (Dkt. No. 17), Plaintiff K.Mizra LLC ("K.Mizra") submits its opening claim construction brief on the disputed claim terms in U.S. Patent Nos. 8,234,705 ("the '705 Patent") and 8,965,892 ("the '892 Patent").

K.Mizra's proposed construction for the '705 Patent claim term "trusted platform module" accounts for general implementations of the module as disclosed in the intrinsic record. In contrast, Defendant Cisco System, Inc. ("Cisco") proposes an unduly narrow construction requiring that the "trusted platform module" must necessarily implement a specific industry standard, rather than according the term its full scope of implementations, consistent with those described in the standard and with the stated purpose of a trusted platform module in the Patent. K.Mizra's proposal remains true to the intrinsic record and purpose of the claim term by covering general implementations including the specific one in Cisco's proposal.

For the '892 Patent, K.Mizra believes that the basic words "electronic document" and "document" need no construction, particularly in light of the claim language. Cisco proposes negative limitations to the claim terms that render the claim language redundant and incorrectly narrow the scope of the claims, based on Cisco's misreading of the patent specification. Cisco's proposal does not offer any actual meaning for the claim terms "electronic document" and "document," but instead inserts exclusionary language that is both superfluous and inconsistent with the intrinsic record. Further, the scope of these terms is clear when read in light of the overall claim and does not require any construction.

Accordingly, K.Mizra respectfully requests that the Court adopt its proposed construction for the claim term at issue in the '705 Patent and give the claim terms at issue in the '892 Patent their plain and ordinary meanings.

II. OVERVIEW OF THE PATENTS-IN-SUIT

A. U.S. Patent No. 8,234,705

The '705 Patent is entitled "Contagion Isolation and Inoculation." ('705 Patent, Ex. A at (54).) It discloses methods and systems for securing a computer network by detecting viruses and/or vulnerabilities on a computer attempting to access a secure network, quarantining the computer by restricting access to the network upon detection of an infestation or vulnerability, and permitting limited access to the protected network for remedying the insecure condition on the computer. ('705 Patent at Abstract, 11:15-12:13.)

Prior art computer network security systems faced considerable challenges with protecting and maintaining up-to-date security software on mobile devices such as employee's personal laptops, which posed significant security risks that could allow attackers or viruses stealth access into a business's network, bypassing IT security measures. (*Id.* at 1:34-38.) While a network security appliance or hardware can adeptly keep out unwanted external intrusions into the network, the most exploitable vulnerabilities of a computer network are the end-user computers that roam throughout various other insecure public and private network domains and then access the presumably secure network day in and day out. (*Id.*)

The '705 Patent closes this loophole by verifying that any device attempting to access a company's network meets its standards for network security and will not introduce dangerous computer programs or viruses into the network. This verification is made by way of an attestation of cleanliness from a trusted computing base associated with a trusted platform module to prevent a forged or falsified report. (*See, e.g., id.* at Claim 1, 13:64-14:12; '705 Patent File History, Jan. 10, 2010 Response, Ex. B at 8.) Furthermore, when "a request is received from a host, e.g., via a network interface, to connect to a protected network, it is determined whether the host is required

to be quarantined. If the host is required to be quarantined, the host is provided . . . limited access to the protected network . . . only as required to remedy a condition that caused the quarantine to be imposed, such as to download a software patch, update, or definition; install, remove, and/or configure software and/or settings as required by a policy; and/or to have a scan or other diagnostic and/or remedial operation performed.” (’705 Patent at 3:8-20.)

B. U.S. Patent No. 8,965,892

The ’892 Patent is entitled “Identity-Based Filtering.” (’892 Patent, Ex. D at (54).) It discloses methods for determining a reputation associated with an electronic document by determining various information relating to the document including an identity of a person associated with the document, the reputation of the person, and the reputation of a group associated with the person. (’892 Patent at Abstract, Claim 1, 2:10-62.)

At the time of the invention, the vast amounts of electronic documents and content on the internet such as PDFs, webpages, and electronic mail accessible via a network address presented a myriad of undesirable content that users encountered. (*Id.* at 1:19-22.) Traditional approaches to filtering such unwanted content fell short, however, as such techniques were solely based on including or excluding certain addresses or uniform resource locators (URLs) associated with the document. *Id.* at 1:19-34. These approaches failed to discriminate between specific content owners or creators of the documents, leading to either inclusion of objectionable content, or exclusion of desirable content. (*Id.* at 1:23-32.)

The ’892 Patent improves upon these conventional techniques for computerized filtering of electronic documents over the internet by determining a reputation of the document. This is achieved by extracting and resolving certain data inherent in the electronic document to determine and correlate the reputation of the author or sender of the document and the reputation of the group

in which he or she may be a member of. (*Id.* at 2:10-62.) For example, the '892 Patent discloses content analysis technology that determines an identity of a person associated with an electronic document, the reputation of a group associated with a person, and an identity reputation associated with the identity based at least in part on the group reputation in order to resolve a reputation of the document. (*Id.* at 2:10-62, Claim 1.)

III. AGREED UPON CONSTRUCTIONS

Patent	Claim Term	Agreed Construction
'705 Patent (claims 1, 12, 19)	"trusted computing base"	Hardware or software that has been designed to be a part of the mechanism that provides security to a computer system
'892 Patent (claims 1, 14, 15)	"identity relating to a person"	Identifier associated with a person such as a user name, user ID, user number, email address, or any other identifier suitable for referring to a person's identity

IV. DISPUTED TERMS AND CONSTRUCTIONS

A. U.S. Patent No. 8,234,705

i. "trusted platform module"

Claim Term	K.Mizra's Proposed Construction	Cisco's Proposed Construction
"trusted platform module" (claims 1, 12, 19)	A secure cryptoprocessor that can store cryptographic keys, which includes but is not limited to a cryptoprocessor that implements the Trusted Platform Module specification from the Trusted Computing Group	A secure cryptoprocessor that implements the Trusted Platform Module specification from the Trusted Computing Group

The parties agree to the extent that the term, "trusted platform module," is a secure cryptoprocessor, but disagree as to whether the cryptoprocessor must necessarily implement the

Trusted Platform Module specification from the Trusted Computing Group. K.Mizra's proposal is entirely consistent with the intrinsic record including all possible cryptoprocessors contemplated by the invention, whereas Cisco's proposal unduly limits the claim term to only a lesser subset of these cryptoprocessors.

A trusted platform module, i.e., a secure cryptoprocessor, is used in the invention of the '705 Patent as an integral part of a novel approach to determine the cleanliness of computers and prevent false reports of such cleanliness. (*See, e.g., '705 Patent at 13:64-14:12; '705 Patent File History, Jan. 10, 2010 Response, at 8.*) By using a secure cryptoprocessor (i.e., a trusted platform module), the invention can avoid falsified attestations. Using "a trusted platform module with a valid digitally signed attestation of cleanliness in detecting an insecure condition are significant innovations, as they can, for example, prevent false reports by ensuring that an attestation of cleanliness is reliable and the result of properly executed checks." ('705 Patent File History, Jan. 10, 2010 Response, at 8.)

The patentee explains in the patent file history that a trusted platform module is a term of art by incorporating a Wikipedia entry which states that:

Trusted Platform Module (TPM) is both the name of a published specification detailing a secure cryptoprocessor that can store cryptographic keys that protect information, ***as well as the general name of implementations of that specification***, often called the 'TPM chip' or 'TPM Security Device' (as designated in certain Dell BIOS settings[1]) . . . Reinforcing the industry adoption of this technology and standardization around the term of art used in the claims, this specification has also been adopted as ISO/IEC standard 11889."

('705 Patent File History, Jan. 10, 2010 Response, at 8 (emphasis added).) Therefore, a person of ordinary skill in the art understood that the trusted platform module can include a number of

different cryptoprocessors that can store cryptographic keys¹, not simply one particular implementation—i.e., the trusted platform module corresponds to any general implementation of such cryptoprocessor as described in, for example, various industry standards and specifications such as the “TPM Specification” or the “ISO/IEC 11889 Standard.” (*Id.*) But the claim term is agnostic with respect to any specific standard or specification, so long as the cryptographic functionality is implemented in a way that utilizes cryptography to prevent falsified reports as taught by the invention. (*Id.* at 7-8; ’705 Patent at 13:64-14:12.)

Cisco’s overly narrow proposal—which would restrict the trusted platform module solely to one implementation, the Trusted Platform Module specification from the Trusted Computing Group—misses this key purpose of the claim term and is unsupported by the broader intrinsic record, which accounts for multiple implementations, standards, and specifications. Accepting Cisco’s proposal would improperly read out other similar implementations of cryptoprocessors the patentee explicitly envisioned, such as the ISO/IEC 11889, which he explained was another standard that adopted the implementation in the Trusted Computing Group standard. (*See, e.g.*, ’705 Patent File History, Jan. 10, 2010 Response, at 8.) As the Federal Circuit has held, “[a] claim construction that excludes the preferred embodiment,” or, as here, other explicitly disclosed embodiments, “is rarely, if ever, correct and would require highly persuasive evidentiary support.”). *Synqor, Inc. v. Artesyn Tech., Inc.*, 709 F.3d 1365, 1378-79 (Fed. Cir. 2013) (internal quotations omitted). K.Mizra’s proposal, on the other hand, includes all embodiments and

¹ For example, a reference cited on the face of the patent by the Patent Examiner also demonstrates that those skilled in the art had a consistent understanding of trusted platform module implementations generally, independent of the Trusted Computing Group specification. *See, e.g.*, ’705 Patent at (56), OTHER PUBLICATIONS; Ex. C, OLS: Linux and trusted computing, Jul. 22, 2005, <http://lwn.net/Articles/144681/>.

disclosed implementations, including the one that Cisco proposes in its construction. Thus, K.Mizra’s proposal, which is the most in line with the intrinsic evidence, should be adopted.

B. U.S. Patent No. 8,965,892

i. “electronic document”

Claim Term	K.Mizra’s Proposed Construction	Cisco’s Proposed Construction
“electronic document” (claims 1, 14, 15)	No construction necessary	The term “electronic document” excludes electronic documents not accessible via a network address, and email

The term “electronic document” consists of two common English words readily understandable to a lay juror and does not require any special definition. *CloudfChange, LLC v. NCR Corp.*, No. 6-19-CV-00513-ADA, 2020 U.S. Dist. LEXIS 124625, at *6 (W.D. Tex. July 15, 2020) (citing *Kroy IP Holdings, LLC v. Safeway, Inc.*, No. 2-12-CV-800-WCB, 2014 U.S. Dist. LEXIS 102136, 2014 WL 3735222, at *2 (E.D. Tex., July 28, 2014)) (finding terms such as “PC workstations” and “point of sale builder software” not needing construction as “none of these terms are difficult technical terms for which a construction would help the jury understand the meaning of the term”). Cisco’s proposed construction attempts to needlessly and incorrectly restrict the scope of the claim term with a negative limitation instead of construing its meaning.

First, there is no need to further define the scope of electronic documents, particularly in light of the claim’s preamble. The preamble of claim 1, for example, adequately clarifies the type of electronic documents that are within the scope of the claim by reciting: a “method for determining a reputation associated with ***an electronic document accessible via a network address.***” As illustrated below, when the preamble phrase provides the antecedent basis for a claim limitation, this Court and the Federal Circuit have found such preamble to limit the claim scope accordingly. *Digital Retail Apps, Inc. v. H-E-B, LP*, No. 6-19-CV-00167-ADA, 2020 U.S. Dist.

LEXIS 11094, at *22 (W.D. Tex. Jan. 23, 2020) (finding the preamble limiting when terms within the claim body rely on the preamble for antecedent basis) (citing *Catalina Mktg. Int'l v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002)).

What is claimed is:

1. A method for determining a reputation associated with an electronic document accessible via a network address, comprising:

determining an identity relating to a person, wherein the identity is associated with the electronic document;
determining that the person is a member of a group, wherein the group is associated with a group-related service and wherein the group is associated with a group reputation;

(’892 Patent at 8:58-67.) Here, Cisco’s improper attempt to limit the scope of the term, electronic document, is superfluous. The preamble is clear on its face that the claim is directed towards the subset of electronic documents that are accessible via a network address. As such, Cisco’s proposal to expressly exclude those electronic documents that are not accessible via a network address from the claim scope is redundant and should be rejected. *See, e.g., TMI Prods. v. Rosen Entm’t Sys., L.P.*, 610 F. App’x 968, 972 (Fed. Cir. 2015) (rejecting claim construction that creates redundancies in the claim language); *see also Victor Co. of Japan, Inc. v. Intervideo, Inc.*, No. A-08-CA-041-SS, 2009 U.S. Dist. LEXIS 133777, at *19-20, 22 (W.D. Tex. July 24, 2009) (rejecting constructions that render claim language redundant and finding that no construction is necessary).

Second, the patentee’s usage of the term is consistent with its plain and ordinary meaning. The patent provides several examples consistent with what both a layperson and a person of ordinary skill in the art would understand to be electronic documents compared to non-electronic documents. It lists examples of electronic documents such as web pages, PDF documents, Flash documents, and emails versus non-electronic documents such as printed documents. (*See, e.g.,*

'892 Patent at 2:15-18.) There is a heavy presumption that this customary meaning applies unless “the patentee (1) acts as his/her own lexicographer or (2) disavows the full scope of the claim term” in the intrinsic record. *Ancora Techs., Inc. v. LG Elecs. Inc.*, No. 1-20-CV-00034-ADA, 2020 U.S. Dist. LEXIS 150002, at *6 (W.D. Tex. Aug. 19, 2020) (citing *Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012)). But the patentee did neither here.

The patentee did not act as his own lexicographer to limit the scope of the term “electronic document” in the manner Cisco suggests. “To act as his/her own lexicographer, the patentee must ‘clearly set forth a definition of the disputed claim term,’ and ‘clearly express an intent to define the term.’” *Ancora*, 2020 U.S. Dist. LEXIS 150002 at *6. Here, the specification of the '892 Patent does not express any intent to redefine the term “electronic documents.” Instead, it merely describes (1) electronic documents that are accessible via a network address and (2) electronic documents that are *not* accessible via a network address. The patent provides examples of an “electronic document that is accessible via a network address such as a web page, a PDF document, and a Flash document,” and conversely, “an electronic document not accessible via a network address,” such as a local file or email that is not accessible via a network address:

FIG. 1 is a diagram of a system for filtering based on identity, according to some embodiments. In this example, a document and/or document metadata **101** is to be filtered. A document refers herein to any electronic document that is accessible via a network address such as a URL. Examples of a document include a web page, a PDF document, and a Flash document. As used herein, a document does not refer to a non-electronic document such as a printed document, nor to an electronic document not accessible via a network address, such as a local file not accessible via a network address, or an email. Document metadata refers herein to any information associated with a document, such as a URL associated with the document.

(*See, e.g.*, '892 Patent at 2:13-21.) The intent of this disclosure was to emphasize the network-accessible nature of electronic documents within the scope of the invention, not to define the term “electronic document” itself. And when the patentee wished to limit the scope of an electronic document, it did so in the preamble, by laying the antecedent basis for the term and limiting it to only those accessible via a network address.

Nor did the patentee’s statements represent a clear disavowal of scope of the claim term. *Ancora Techs., Inc. v. LG Elecs., Inc.*, No. 1-20-CV-00034-ADA, 2020 U.S. Dist. LEXIS 150002, at *6-7 (W.D. Tex. Aug. 19, 2020). Nothing in the patent suggests that “electronic documents” conceptually exclude those documents that are inaccessible via a network address. Rather, certain electronic documents are accessible via a network address, while certain others are not. The patentee describes one category of electronic documents that are accessible via a network address, and also provides contrasting examples of electronic documents that are not accessible via a network address, such as files or emails that are locally stored. ('892 Patent at 2:19-21.) But as to the umbrella concept of electronic documents, both an email that *is* accessible via a network address (i.e., stored on a server) and an email *not* accessible via a network address (i.e., stored locally) are different sub-categories of electronic documents.

Absent a clear and unmistakable disavowal, Cisco’s proposal to narrow the meaning of electronic documents to exclude *all* emails should be rejected. *See Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1123 (Fed. Cir. 2004) (refusing to impose a negative limitation because the patent did not present a “clear and unmistakable disavowal”). No construction of the term “electronic document” is necessary as it should be given its plain and ordinary meaning.

ii. “document”

Claim Term	K.Mizra’s Construction	Cisco’s Construction
“document” (claims 1, 5, 6, 14, 15)	No construction necessary	The term “document” excludes non-electronic documents, electronic documents not accessible via a network address, and email

Like the term “electronic document,” the term “document” also need not be construed given that the preamble as well as the surrounding claim language adequately establishes the scope of the claim term. As illustrated below, the recitation of the term “document” in the context of claim 1, for example, is understood as referring to electronic documents accessible via a network address. Imposing a negative restriction on the term as Cisco proposes is not only redundant and improper as a matter of law, but also suffers from an incorrect interpretation of the patent specification—i.e., as addressed (and rebutted) above, Cisco argues that documents exclude *all* emails, rather than only locally stored emails that are not accessible via a network address.

What is claimed is:

1. A method for determining a reputation associated with an electronic document accessible via a network address, comprising:
 - determining an identity relating to a person, wherein the identity is associated with the electronic document;
 - determining that the person is a member of a group, wherein the group is associated with a group-related service and wherein the group is associated with a group reputation;
 - determining an identity reputation, wherein the identity reputation is associated with the identity and wherein the identity reputation is based at least in part on the group reputation; and
 - determining a document reputation, wherein determining the document reputation uses the identity reputation.

Claim 1, for example, as shown above, is directed towards documents that are electronic and accessible via a network address. (See '892 Patent at 8:58-9:6.) As discussed above, when reading the claim in its totality, including the preamble, it is clear that all instances of the word, “document,” refer to electronic documents accessible via a network address. Thus, Cisco’s proposal is redundant and should be rejected at least on that basis alone. As also discussed above, Cisco’s proposal should be rejected to the extent that it excludes *all* emails from the scope of the claim based on an incorrect interpretation of the patent specification.

Moreover, Cisco’s proposal is an improper attempt to narrow the claim scope to a particular embodiment. *Comark Commc’ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1187 (Fed. Cir. 1998) (“particular embodiments and examples appearing in the specification will not generally be read into the claims.”). Indeed, the patentee explains that these descriptions are offered in the context of an “example,” “according to some embodiments.” (*Id.* at 2:10-11.) He also explains that a “description of one or more embodiments of the invention is provided” and that “[t]he invention is described in connection with such embodiments, but the invention is not limited to any embodiment. The *scope of the invention is limited only by the claims*, and the invention encompasses numerous alternatives, modifications and equivalents.” *Id.* at 1:61-2:1. Such example embodiments in the specification should not be imported into a special definition for the claim term. See *Sumitomo Dainippon Pharma Co. v. Emcure Pharm. Ltd.*, 887 F.3d 1153, 1159 (Fed. Cir. 2018) (quoting *Johnson Worldwide Assocs., Inc. v. Zebco Corp.*, 175 F.3d 985, 992 (“[M]ere inferences drawn from the description of an embodiment of the invention cannot serve to limit claim terms.”)). Even when a patent specification describes only one embodiment, descriptions of that embodiment do not limit the claim scope. *Pisony v. Commando Constr., Inc.*, No. W-17-CV-00055-ADA, 2019 U.S. Dist. LEXIS 31524, at *10-11 (W.D. Tex. Jan. 23, 2019) (finding claim

scope not limited to a vertical mast even when all figures of the patent showed only a vertical mast). Thus, Cisco's construction should be rejected as no construction of the term "documents" is necessary.

Date: May 26, 2021

Respectfully submitted,

FOLIO LAW GROUP PLLC

/s/Cliff Win, Jr.

Cristofer I. Leffler, WA Bar No. 35020

Cliff Win, Jr., CA Bar No. 270517

Folio Law Group PLLC

14512 Edgewater Lane NE

Lake Forest Park, WA 98155

T: (206) 512-9051

Email: cris.leffler@foliolaw.com

Email: cliff.win@foliolaw.com

Joseph M. Abraham, TX SB No. 24088879

Law Office of Joseph M. Abraham, PLLC

13492 Research Blvd., Suite 120, No. 177

Austin, TX 78750

T: (737) 234-0201

Email: joe@joeabrahamlaw.com

Attorneys for K.Mizra LLC

PROOF OF SERVICE

**K.Mizra LLC v. Cisco Systems, Inc.
Case No. 6:20-CV-01031-ADA**

On May 26, 2021, I served a true copy of the following document(s) described as
PLAINTIFF K.MIZRA LLC'S OPENING CLAIM CONSTRUCTION BRIEF on the interested
parties in this action as follows:

Via Email:

Elizabeth Brannen
elizabeth.brannen@strismaher.com

Kenneth Halpern
khalpern@strismaher.com

Melissa Richards Smith
melissa@gillamsmithlaw.com

Dated: May 26, 2021

/s/Cliff Win, Jr.
Cliff Win, Jr.